Consolidated Technology Services • WA

Service Inquiry
Rights Management Service

July 2012

Overview and Potential Benefits

Active Directory (AD) Rights Management Service (RMS) is a service that uses encryption and policies to limit what access and actions are allowed with a target email or document. RMS consists of a server application (RMS Core Cluster) that is in communication with client applications on user's workstations. This client software is included with the newer Microsoft operating systems and Office Suites and is available for download from Microsoft for many of the older supported products.

Only one RMS Core Cluster can be deployed per AD forest, making a good case for deploying it as an 'enterprise service offering' in the Enterprise Active Directory (EAD) forest used by most (but not all) State Government agencies. Its functionality can be extended to other forests and entities using Microsoft Federation Gateway and/or Active Directory Federation Services (ADFS), but that is outside the scope of this analysis.

Features of RMS include:

- Limit document and email access to defined AD individuals or groups.
- Limit document access (when a document can be opened, where it can be opened, set expiration).
- Limit document actions (printing, copying, editing, reading, forwarding or deleting).
- Policies can be assigned to individual emails or documents or to contents of a file folder.
- 'Out of the box' support for files, email, SharePoint. Can be extended to work with other applications using an RMS Software Development Kit.
- Implementation in Exchange that maintains proper rights even when email is viewed 'off-line'.
- If an RMS-protected document is inadvertently sent to an entity outside of the EAD, that document will not be accessible.
- Connectors are available for WaSERV (Enterprise Vault) and BlackBerry Services. There may be additional costs for these connectors.
- Persistent document protection. Even after the document is opened, the policy still protects the document – unlike encrypted documents, that once unencrypted, are no longer protected.

CTS Effort to Deploy and Support:

A minimum installation would include three servers (two in Olympia and one in a remote site) and a SQL Cluster that is isolated due to the security information that is stored on the database. SQL should be replicated to a remote site using synchronous replication as a loss of licensing configuration would result in a loss of access to data.

Estimated Time to Implement: A more complete understanding of resource and business requirements will determine the project timeline. An Enterprise RMS installation may require

assistance from Microsoft to implement due to the complexity of the EAD forest. A standard set of policies will also need to be developed and implemented with collaboration from agency partners.

Deployment: Only one RMS Cluster can be installed in the EAD Forest. RMS would therefore be a root service of the Enterprise Active Directory and would be managed by the Root Administrators for the EAD Forest.

Support and Maintenance: Maintenance of the production and pre-production RMS systems would include creating templates and policies, publishing templates, managing the template library for the Enterprise, patching, monitoring, SQL maintenance and troubleshooting, troubleshooting issues with the RMS system itself, certification of client machines, and working with agencies to test and implement customer templates and policy requests.

Processes and Custom Templates: A process for requesting, testing, approving and implementing customer templates requested by agencies will need to be developed and managed by CTS. This could potentially be overseen by the Forest Application Developers Group (FAD), the Forest Resource Group (FRG) and the EAD Steering Committee.

Agency Support Responsibilities:

Client Installation and Troubleshooting – Agencies may need to install RMS clients on some older operating systems. RMS has a native client included in Vista, Windows 7, Windows 2008 and IE 8.0 and Office 2003 and above. Other clients can be downloaded from Microsoft. In addition, each computer will need to be enabled in order to receive a public and private key in order to access RMS content. This will be an ongoing maintenance task for agencies to troubleshoot and maintain this relationship between the client and the RMS system in order for the user to access RMS encrypted data.

User Training: User training will be required on how to use RMS templates, how to troubleshoot issues with RMS, and to be clear that RMS controls will only be honored for recipients within the EAD forest.

Developing and Testing Custom Templates: Agencies may have a need to deploy custom templates and/or enable custom applications to use RMS. This would be their responsibility, and would require that they have a pre-production environment available for testing (many already do). CTS would need to assist with the testing of the templates, but would not be responsible for troubleshooting or assisting in development of these templates.

Estimated Cost:

System Cost: A basic installation of Rights Management Service limited to the EAD forest would require three Windows 2008 R2 Servers behind a hardware load-balancer and a two-node SQL cluster with a replication partner in a remote site. This system could support approximately 100 – 200 requests from clients per second. The system could be scaled out by adding additional virtual servers to support a larger implementation. This is an add-on service and does not require a separate software license. Since there is a potential for loss of access if the system fails, a highly-available, redundant and site-distributed installation is highly recommended and is included in the estimated pricing.

Based on high-level scoping, the estimated cost of the RMS servers and the SQL Cluster and infrastructure (network, firewalls and load balancer) is approximately $6,000 per month. This cost will change based on further requirements gathering and design.

Support Costs: From a preliminary investigation, RMS appears to be a potentially time-consuming application to support. RMS requires several different support roles – Enterprise Admin, Template Administrator, and RMS Auditor. These roles can be distributed across several people, but all roles would need to remain in CTS, due to the root-level installation and access required. All templates will need to be enabled by CTS. There are no default templates included with the product. A standard set of templates will need to be developed and tested. It is estimated that ongoing support would require a full FTE. Initial support would be much higher during deployment and until a set of basic templates is established.

The estimated cost for on-going support is approximately $12,000 per month.

Total Cost Estimate: $18,000 per month

Additional Technical Detail:

The RMS Core Cluster consists of several components: A root certification server and licensing server, additional certification and licensing servers, and a SQL Database. Only one Root Certification Server can be installed in a single forest. Microsoft SQL is a requirement for a production installation of RMS.

The RMS Root Certification Server is different from a Microsoft Certificate Server and authorizes clients into the RMS system. The RMS Licensing Server provides licenses that allow the document to be accessed depending on the policy and must be accessible in order to decrypt the document.

RMS is installed on a Windows 2008 Server and does not require additional client access licenses or software licenses. RMS runs on top of IIS and is a likely candidate for installation on

virtual servers. RMS Servers are installed in a “cluster” for redundancy and high availability. In addition, the configuration and licensing is stored on a Windows SQL Server. The SQL Server should be highly available and redundant as any loss of licensing data could result in a loss of access to data that has been encrypted by the RMS system. RMS should be managed in the same way as a Certificate Authority, as its function in Active Directory is very similar.